

1. The first step is to identify the key components of the system. This includes understanding the hardware, software, and data involved. For example, in a web application, this might involve identifying the server, database, and client-side code.

2. The second step is to analyze the system's behavior. This involves observing how the system responds to different inputs and outputs. This can be done through manual testing or automated testing tools.

3. The third step is to identify potential vulnerabilities. This involves looking for weaknesses in the system that could be exploited by an attacker. This can be done through a variety of techniques, including code review, penetration testing, and vulnerability scanning.

4. The fourth step is to develop a plan to address the identified vulnerabilities. This involves determining the best way to fix each vulnerability and prioritizing the fixes based on their severity.

5. The fifth step is to implement the plan. This involves making the necessary changes to the system and testing the fixes to ensure they are effective.

6. The sixth step is to monitor the system for future vulnerabilities. This involves regularly checking the system for new vulnerabilities and updating the security plan as needed.

7. The seventh step is to document the findings and actions taken. This involves creating a report that details the results of the audit and the steps taken to address the vulnerabilities.

8. The eighth step is to communicate the findings to the relevant stakeholders. This involves sharing the report with the system owners, developers, and other interested parties.

9. The ninth step is to review the audit process. This involves reflecting on the audit and identifying areas for improvement for future audits.

10. The tenth step is to repeat the process. This involves conducting regular audits to ensure the system remains secure over time.

Andre Boyce

3623

[illegible]

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner

[illegible]